CLAIMS

What is claimed is:

1. A multiple modulus selector comprising:

a modulus recoder for receiving a n-bit modulus number M and a previous sum and a current partial product and producing a selection signal; and

a multiplexer for receiving four inputs –M, 0, M, and 2M and selecting one of the inputs based on the selection signal.

2. The multiple modulus selector of claim 1, wherein the input –M is obtained by inverting the modulus number M.

3. The multiple modulus selector of claim 1, wherein the input 2M is obtained by shifting the modulus number M.

4. The multiple modulus selector of claim 1, wherein the modulus number M is stored in a register.

5. The multiple modulus selector of claim 1, wherein the modulus recoder further produces a multiple modulus negation indicating signal NEG_MM, wherein the negation indicating signal is input to an accumulator.

6. The multiple modulus selector of claim 1, wherein the n-bit modulus number M includes a next least significant bit M[1] and the previous sum and current partial product is a two bit number , including a least significant bit $SPP_I[0]$ and a next least significant bit $SPP_I[1]$.

7. The multiple modulus selector of claim 1, wherein the selection signal includes two bits SEL_MM [1:0].

8. An accumulator, comprising:

a plurality of compressors for operating in a carry save mode, each of the plurality of compressors receiving a multiple modulus, a partial product, a corresponding current sum, and a corresponding current carry and producing a corresponding next sum and a corresponding next carry;

a sum register for receiving the corresponding next sum from each of the plurality of compressors and outputs a corresponding updated current sum ; and

a carry register for receiving the corresponding next carry from each of the plurality of compressors and outputs a corresponding updated current carry.

9. The accumulator of claim 8, wherein the sum register and carry register are separate registers.

10. The accumulator of claim 8, wherein the multiple modulus is produced from a modulus.

11. The accumulator of claim 10, wherein n is the bit length of the modulus and the plurality of compressors include n+3 compressors.

12. The accumulator of claim 11, wherein the modulus is stored in an n-bit register.

13. The accumulator of claim 8, wherein the partial product is produced from a multiplicand and a multiplicator.

14. The accumulator of claim 13, wherein n+1 is the bit length of the multiplicand.

15. The accumulator of claim 14, wherein the multiplicand is stored in an (n+1)-bit register.

16. The accumulator of claim 13, wherein if n is even, then n+2 is the bit length of the multiplicator and if n is odd, then n+1 is the bit length of the multiplicator.

17. The accumulator of claim 16, wherein if n is even, the multiplicator is stored in an (n+2)-bit register and if n is odd, the multiplicator is stored in an (n+1)-bit register.

18. The accumulator of claim 8, wherein each of the plurality of compressors is a 5:2 compressor.

19. The accumulator of claim 8, a first group of the plurality of compressors further receiving a compensating word to produce the corresponding next sum and the corresponding next carry.

20. The accumulator of claim 19, wherein the first group of the plurality of compressors are full compressors.

21. The accumulator of claim 19, wherein a second group of the plurality of compressors does not receive the compensating word.

22. The accumulator of claim 21, wherein the second group of the plurality of compressors are reduced compressors.

23. The accumulator of claim 8, wherein each of the partial product and the multiple modulus are n+2 bits.

24. The accumulator of claim 19, wherein the compensating word is 2 bits.

25. The accumulator of claim 19, wherein the full compressor is composed of three full adders.

26. The accumulator of claim 22, wherein the reduced compressor is composed of one half adder and two full adders.

27. The accumulator of claim 8, further comprising:

a carry propagate adder for receiving a finally updated current sum and a finally updated current carry and outputs a final sum in normal number representation; and

a final register for storing the final sum.

28. The accumulator of claim 8, wherein the plurality of compressors operate in both the carry save mode and a carry propagate mode.

29. The accumulator of claim9, wherein the carry save mode and the carry propagate mode are determined by a control signal.

30. The accumulator of claim 28, a first group of the plurality of compressors further receiving a compensating word to produce the corresponding next sum and the corresponding next carry.

31. The accumulator of claim 30, wherein the first group of the plurality of compressors are full compressors.

32. The accumulator of claim 30, wherein a second group of the plurality of compressors does not receive the compensating word.

33. The accumulator of claim 32, wherein the second group of the plurality of compressors are reduced reconfigurable compressors.

34. The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes:

a multiplexer group for reconfiguring each of the reduced reconfigurable compressors to operate in both the carry save mode and the carry propagate mode.

35. The accumulator of claim 34, wherein each multiplexer group includes three 2:1 multiplexers.

36. The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes a multiplexer group which reconfigures the reduced reconfigurable compressor to operate in either the carry save mode or the carry propagate mode according to the control signal.

37. The accumulator of claim 36, where the carry save mode includes a first signal flowing from a middle full adder of a current compressor to a bottom full adderof the current compressor, a second signal flowing from -a top adder of -a lower compressor to the-bottom full adder of the current compressor, and a third signal flowing from a middle full adder of the lower compressor to the bottom full adder of the currentcompressor.

38. The accumulator of claim 36, where the carry propagate mode includes a first signal flowing from a bottom full adder of a lower compressor to the multiplexer group of a higher compressor and a second signal flowing from the multiplexer group of the higher compressor to a bottom full adder of the higher compressor.

39. The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes:

a multiplexer group for receiving a sum of a middle full adder of the current compressor, a corresponding updated current carry of a lowercompressor, a first and second secondary output of the lowercompressor, the updated current sum of the currentcompressor, and the corresponding next carry of the lowercompressor and outputting first through third outputs.

40. The accumulator of claim 31, wherein the full compressor is composed of three full adders.

41. The accumulator of claim 33, wherein the reduced reconfigurablecompressor is composed of one half adder ,two full adders and three 2:1 multiplexers.

42. A Montgomery multiplier comprising:

a multiple modulus selector, wherein the selector selects a multiple modulus from one of –M, 0, M, and 2M, where M is an n-bit modulus number;

a booth recoder, wherein the booth recoder provides first values used to obtain a partial product value; and

an accumulator, wherein the accumulator accumulates second values obtaining a result for the Montgomery multiplier.

43. The multiplier of claim 42, further comprising:

a modulus number register, wherein the modulus number register holds a modulus value;

a multiplicand register, wherein the multiplicand register holds a multiplicand value;

a multiplier register, wherein the multiplier register holds a multiplier value;

an AND gate, where the AND gate combines two values derived from the multiplicand value and the multiplier value; and

two adders, wherein the adders combine values from the accumulator and the AND gate producing a combined value, where the multiple modulus selector inputs the combined value.

44. A method of multiple modulus generation, comprising:

receiving a modulus;

receiving a previous sum and a current partial product, wherein the modulus and the previous sum and a current partial product are used to produce multiple modulus values of -M, 0, M, and 2M.

45. The method of claim 44, further comprising receiving only a portion of the modulus, the portion being the second least significant bit of the modulus.

46. The method of claim 44, further comprising receiving only a portion of the previous sum and a current partial product, the portion being the two least significant bits of the previous sum and a current partial product.

47. The method of claim 44, further producing a selection signal, where the selection signal is used to select a value of the produced multiple modulus values.

48. The method of claim 47, further producing a multiple modulus negation indicating signal, where the modulus negation indicating signal is used to produce a complement of the selected value.

49. A method of partial product generation, comprising:

receiving a multiplier number; and

generating a partial product selection signal, a partial product enabling signal, a partial product negation indicating signal to produce at least one partial product value.

50. The method of claim 49, further comprising shifting the multiplier number by two bits.

51. A method of accumulating, comprising:

receiving a plurality of multiple modulus, partial products, corresponding current sums, and corresponding current carries for producing a corresponding next sum and next carry;

generating updated current sums and updated current carries;

iterating the receiving and generating steps until a multiplier operand is consumed to generate a result in redundant representation; and

performing carry propagation addition to generate a result in normal representation.

52. The method of claim 51, wherein the step of iterating is carry save addition performed by a carry save adder.

53. The method of claim 51, wherein the step of performing is carry propagation addition performed by a carry propagation adder.

54. The method of claim 53, further comprising the step of generating a switching signal.

55. The method of claim 54, further comprising switching between carry save addition and the carry propagation addition using the switching signal.

56. A method of performing radix 2^N Montgomery multiplication, where N>1, comprising;

receiving a multiplicand, a modulus, and a multiplier;

performing carry save addition on a plurality of inputs related to the multiplicand, modulus, and multiplier to generate a result in redundant representation; and

performing carry propagation addition to generate a result in normal representation.

57. The method of claim 56, wherein the carry save addition is performed by a carry save adder and the carry propagation addition is performed by a carry propagation adder.

58. The method of claim 56, wherein the carry save addition and the carry propagation addition is performed by an accumulator.

59. The method of claim 56, further comprising the step of generating a switching signal.

60. The method of claim 59, further comprising switching between the carry save mode and the carry propagation mode using the switching signal.

61. A method of performing radix 2^N Montgomery multiplication, where N>1, comprising;

receiving a multiplicand, a modulus, and a multiplier;

performing accumulation in carry save mode on a plurality of inputs related to the multiplicand, modulus, and multiplier to generate a result in redundant representation; and

performing conversion in carry propagation mode on the result in redundant representation to generate a result in normal representation.